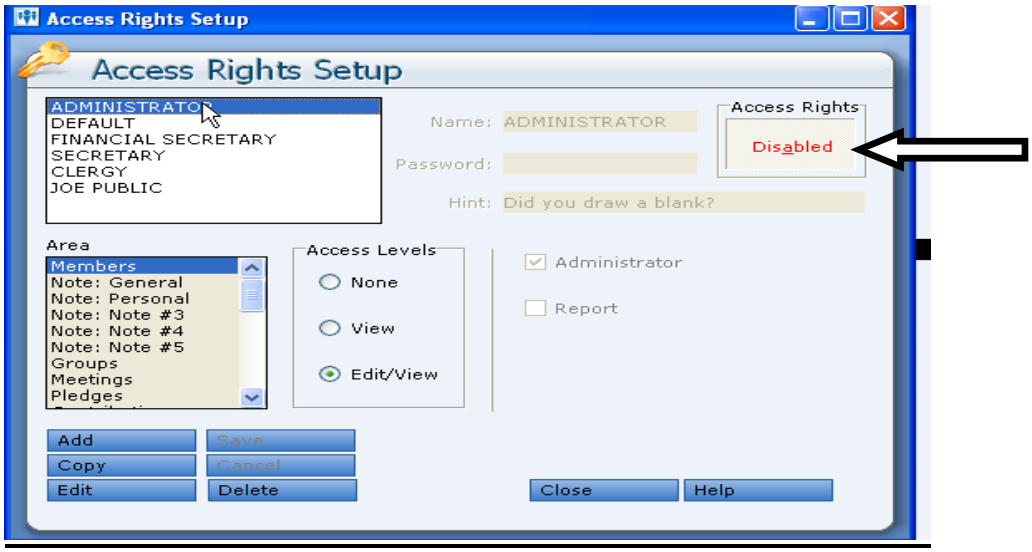
ACCESS RIGHTS SETUP

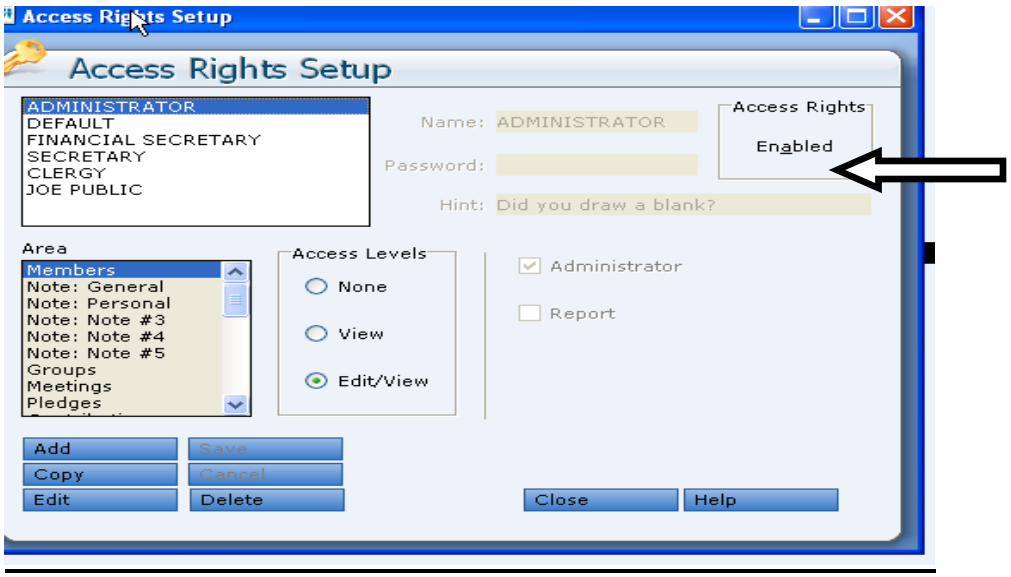
Enabling and disabling access rights

Access rights are initially disabled. In addition to setting up access rights, you need to enable their use for the data set.



To enable access rights,

- In the **Access Rights Setup** dialog box set the **Access Rights Enabled/Disabled** button so that it is raised and labeled **Enabled.**



.

To disable password protection,

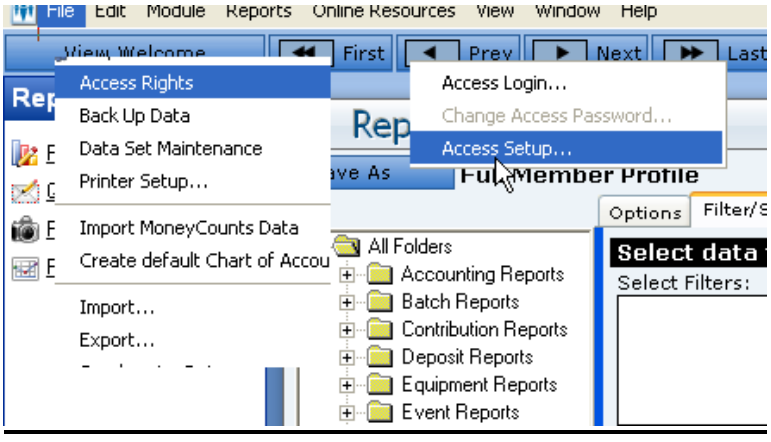
- Return to the **Access Rights Login Administration** dialog box and set the Access Rights Enabled/Disabled button so that it is depressed and labeled **Disabled**.

> **Tip** : Access rights can be enabled or disabled at any time, but the restrictions or lack of them apply to all users. (You can't require some users to log in with a password while others bypass that step.)
>
> **Only Administrators can enable or disable access rights.**

Deleting Access rights

You may want to delete an access name and associated access rights, especially in the case where one of the users of the program leaves the organization or will no longer be responsible for working with the program.

1. From the File menu, select **Access Rights** then **Access Rights Setup**.
2. In the dialog box, Click to select the Access name you no longer need
3. Click Delete. (The access name is removed from the data set.)



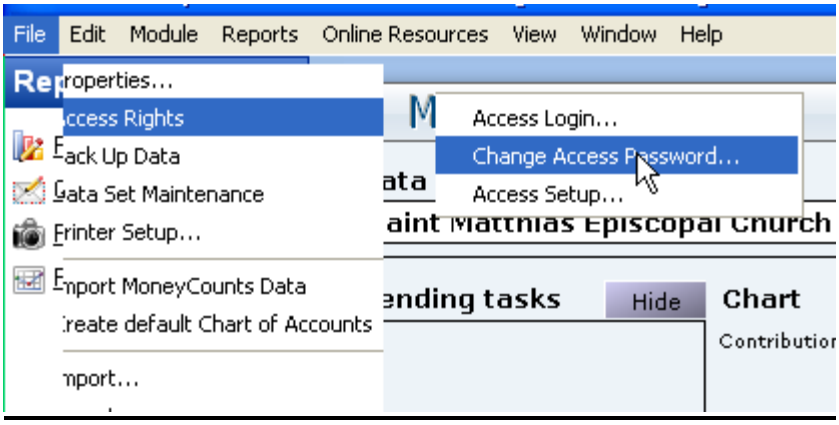
> **Tip**: Only an Administrator can delete a password.
>
> NOTE: The Administrator and Default access names provided by Membership Plus cannot be deleted.

Changing a password

For enhanced security, you may want to change your password periodically.

To change your password

1. From the **File menu**, choose **Access Rights**, and then choose **Change Access Password** from the submenu to open the **Change Access Rights Password** dialog box.



2. Enter your current password.

3. Enter your new password, and then retype it to confirm it.

4. Enter a new hint, if desired.

5. Click **OK** to return to your previous program location.

> **Tip**: Administrators can change passwords in the Access Rights Login Administration dialog box.

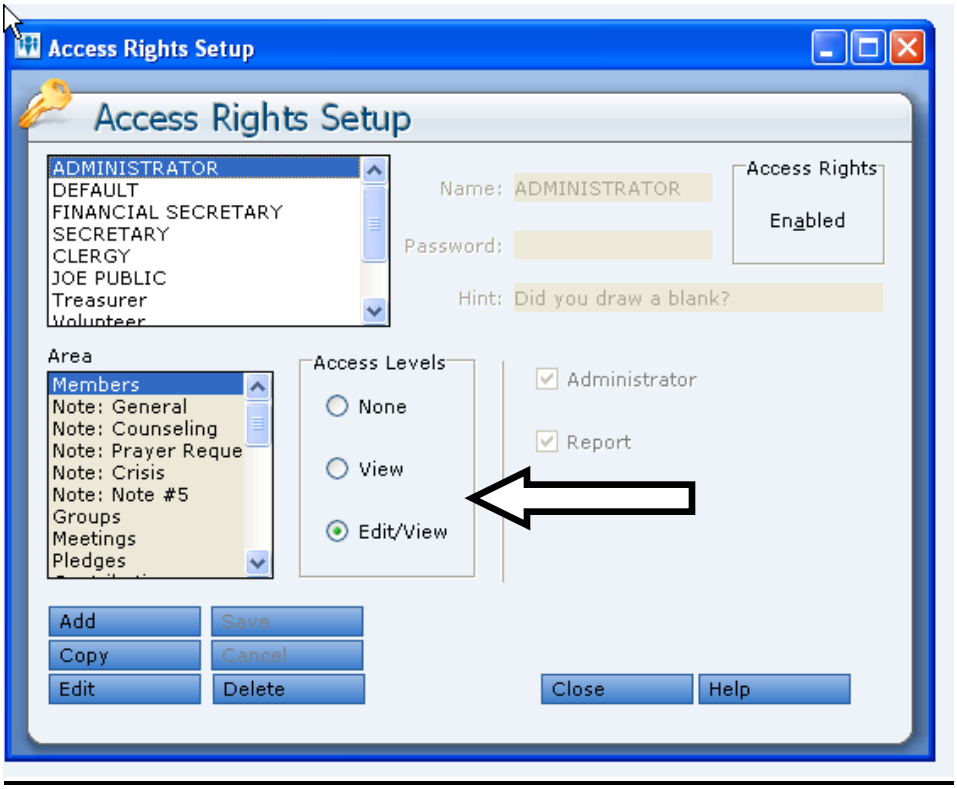
Levels of Access

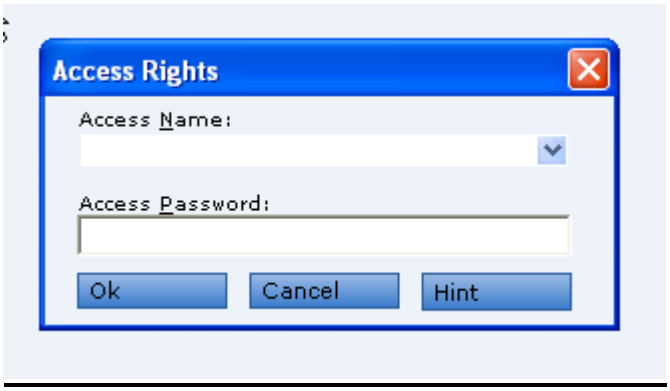
For each restricted user of a data set, you can set access to various areas of the program at the following levels:

- **None**— this level allows the user any access to the specified area of the program. When access rights are set up and the user has logged in, options that are not available to this user are dimmed in the menu and toolbar. Page buttons within modules also may be dimmed, as appropriate. The restricted user also cannot run reports for data related to this area of the program; the report types are unavailable in the Report Generator.

- **View**—this level allows the user to view data that has been entered in the program, but he or she cannot add, modify, or delete records.

- **Edit/View**—this level allows the user full access to data for the specified area.





Logging in with your access name and password

- If access rights are enabled for a data set, you'll have to enter your access name and password each time you open that data set. Once the data set is open, a different user can log in to access the areas of the program to which he or she is entitled.

To log in when the data set is first opened,

- Select your Access Name from the pick list in the Access Rights dialog box, and then enter your password. Click OK to proceed.

To log in as a different user,

1. From the File menu, choose Access Rights, and then choose Access Login from the submenu.
2. Select your access name and enter your password in the Access Rights dialog box and click OK.

Restricting specific areas

You can use access rights to restrict access to only those areas that the user of the access name needs to see. For example, the church secretary might have access to the member and meeting records, but only the treasurer has access to the financial records. Access can be restricted to the following areas of the program:

- Members—Restricts access to information in the various members modules (individuals, families, and organizations.

- Notes—Restricts access to notes entered for members. You can set separate restrictions for each note type, if necessary (as in the case where general information is entered on some pages but confidential information on another).

- Groups—Restricts access to information in the Groups module.

- Meetings—Restricts access to information in the Meetings module.

- Pledges—Restricts access to pledge information entered in the Pledges module (and viewable in the Member Browser).

- Contributions—Restricts access to pledge information entered in the Contributions module (and viewable in the Member Browser).

- Visitation—Restricts access to information in the Visitation Module.

- Scheduler—Restricts access to information in the Room and Equipment Scheduler Module.

- Event Registration—Restricts access to information in the Event Registration Module.

- Backup—Restricts the user's ability to back up the data set.

- Restore—Restricts the user's ability to restore a backed up data set (preventing potential accidental overwriting of data).

- Archive—Restricts the user's ability to archive a data set.
- Import—Restricts the user’s ability to Import information into the data set.
- Export—Restricts the user’s ability to Export information out of the data set.
- Search/Replace—Restricts the user’s ability to Search/Replace data in the data set.
- Surveys—Restricts access to information in the Surveys module.
- Workflow—Restricts access to information in the Workflow module.
- Progress Tracker—Restricts access to information in the Progress Tracker module.
- Accounts—Restricts access to information in the Accounts module.
- Transactions—Restricts access to information in the Transaction module.
- Payees—Restricts access to information in the Payees module.
- Auto Tasks Setup—Restricts access to information in Auto Tasks Setup.
- Auto Tasks Process—Restricts access to information in Auto Tasks Processing.

Tip: When access to a specific area is restricted or denied, the user also cannot generate reports for that area of the program; those report types are unavailable in the Report Generator.